REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
	Technical Report	-

4. TITLE AND SUBTITLE
High-Speed Quantum Key Distribution Using Photonic Integrated Circuits

5a. CONTRACT NUMBER
W911NF-10-1-0416

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
0D10BH

6. AUTHORS
Dirk Englund, Karl Berggren, Jeffrey Shapiro, Chee Wei Wong, Franco Wong, Gregory Wornell

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Columbia University
615 West 131 Street
Room 254, Mail Code 8725
New York, NY 10027 -7922

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
58496-PH-DRP.15

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
The goal of this program is to increase the private information capacity of optical channels. Here we report on the theoretical and experimental progress, including the development and implementation of a large-alphabet quantum key distribution protocol that extends pulse position modulation encoding to quantum key distribution. We have shown security of this protocol against collective attacks. We also describe finite-key length security analysis.

15. SUBJECT TERMS
quantum key distribution, cryptography, photonic integrated circuits

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dirk Englund
UU	UU	UU	UU		19b. TELEPHONE NUMBER 617-324-7014

Report Title

High-Speed Quantum Key Distribution Using Photonic Integrated Circuits

ABSTRACT

The goal of this program is to increase the private information capacity of optical channels. Here we report on the theoretical and experimental progress, including the development and implementation of a large-alphabet quantum key distribution protocol that extends pulse position modulation encoding to quantum key distribution. We have shown security of this protocol against collective attacks. We also describe finite-key length security analysis.

High-Speed Quantum Key Distribution Using Photonic Integrated Circuits

Abstract

The goal of this program is to increase the private information capacity of optical channels. Here we report on the theoretical and experimental progress, including the development and implementation of a large-alphabet quantum key distribution protocol that extends pulse position modulation encoding to quantum key distribution. We have shown security of this protocol against collective attacks. We also describe finite-key length security analysis.

Contents

1 Introduction

There has been rapid progress in developing optical quantum technologies that address unsolved problems in communications, computation, and metrology. Quantum key distribution now makes it possible to transmit information with absolute, unconditional security. These technologies require sophisticated electro-optic circuits, which are presently implemented in large custom-made bulk optics. There now exists an opportunity to translate optical quantum technologies from meter-sized table-top experiments to scalable sub-mm monolithic photonic integrated chips (PICs), leveraging recent advances in integrated optics. We combine quantum information processing (QIP) and PIC technology and a quantum photonic integrated chip (QPIC) architecture, offering densely integrated optical and electronic circuits into a rapidly reconfigurable platform.

High-dimensional quantum key distribution (QKD) [1] allows two parties, Alice and Bob, to establish a secure cryptographic key at a potentially higher rate than that afforded by standard, two-dimensional QKD protocols [2, 3]. When the photonic states are described using a high-dimensional Hilbert space, more than one bit of information can be generated when a single photon is detected. Additionally, increasing the dimension of a QKD protocol provides greater resilience to noise [4]. High-dimensional QKD protocols have been implemented by encoding information in various photonic degrees of freedom, including position-momentum [5], time [6, 7, 8, 9], energy-time [10], and orbital angular momentum (OAM) [11, 12, 13]. Dispersive optics QKD (DO-QKD) is a high-dimensional QKD protocol [14] that uses energy-time entanglement of pairs of photons.

We are employing the QPIC architecture to implement a novel high-dimensional dispersive optics quantum key distribution (DO-QKD) protocol which offers orders of magnitude speed-up in secure communication rate compared to previous QKD implementations. The DO-QKD protocol enables the generation of a secret key between two parties Alice and Bob using high-dimensional photon encoding that enables information capacity in excess of 10 bits per photon. Working at the low-energy limit of secure communication, we will also investigate how telecom technology can be leveraged to approach the classical information capacity of optical channels under bandwidth and optical power constraints.

2 Dispersive Optics QKD Protocol

Numerous degrees of freedom of photons have been investigated, including position momentum, time, energy time, and orbital angular momentum (OAM). Because we desired a protocol that is maximally compatible with modern-day fiber communications systems, we focused on the use of temporal encoding of information. Using a high-dimensional alphabet, the DO-QKD protocol is closely analogous to pulse position modulation (PPM) to maximize the secret-key capacity under technical constraints such as limited numbers of photon produced or limited number of detector clicks per unit time. We have now completed a thorough analysis of the DO-QKD protocol, proving security against collective attacks. To our knowledge, this is the first security proof for a high-dimensional QKD protocol with specific physical realization of the qudits. We have so far analyzed security in the asymptotic limit of infinite key length [15] and are working on an extension of the protocol to capture finite key length effects, to be discussed in Section 2.1 below. The approach employed provides a general framework for proving the security of protocols employing single photons in continuous Hilbert spaces using measures of the covariance matrix. Although we focus the discussion on a scheme employing entangled photon pairs generated by Alice at random times by spontaneous parametric down-conversion (SPDC) and sent to Bob over a quantum channel, we have also developed variations of the scheme that employ single-photon sources or weak classical light. We estimate that practical implementations could reach a secret-key capacity of > 4bits per character of distilled key (bpc) with transmission across over 200 km in fiber. We are currently extending the scheme to also make use of polarization and frequency degrees of freedom to scale up the number of bits per photon.

2.1 Finite-key analysis for arbitrary basis selection probabilities

The security proof for DO-QKD presented in [14] relied on the asymptotic limit: Alice's and Bob's keys were assumed to be infinitely long. We now show security for finite-length keys. To do this, we combine elements of finite-key security proofs [16, 17, 18, 19, 20, 21] with the existing security analysis for DO-QKD. We also allow for asymmetric basis selection [22] to increase the efficiency of the protocol by increasing the probability that Alice and Bob measure in the same bases—a consideration that was unecessary in the asymptotic limit.

In the earliest QKD protocols [2, 3, 23], Alice and Bob selected between the two measurement bases with equal probabilities, limiting the efficiency to at most 50%. It was later suggested [22] that the efficiency of a QKD protocol could be increased asymptotically to 100% if Alice and Bob choose one measurement basis with a greater probability than the other, thereby increasing the likelihood that Alice and Bob will make measurements in the same basis. Furthermore, Lo *et al.* also showed that equal basis selection probabilities are not necessary to prove the security of a QKD protocol [22].

If an eavesdropper, Eve, were aware of Alice and Bob's basis choice probabilities, she could use that information to her advantage: By choosing to eavesdrop in the dominant basis, she could gain more information while remaining undetected. In order to prevent this, Alice and Bob must slightly modify their protocol: They divide their data according to the measurement basis used, and they estimate parameters separately for each basis.

When implementing DO-QKD using asymmetric basis selection, we assume that Alice and Bob choose to measure in the 'time basis' with probability $p > 1/2$; that is, Alice and Bob apply dispersion less than half of the time. Asymmetric basis selection can benefit the key generation rate, as it allows the lossy dispersive elements to be used less frequently. The exact value of p is chosen along with other parameters to optimize the secure key capacity as described below.

2.2 Finite-size effects on secure key capacity

Outside the asymptotic limit, a QKD protocol can never be completely secure. Instead, a protocol can only be ε-secure, where ε is the tolerated failure probability of the entire protocol. The security parameter ε is the sum of the failure probabilities of each stage of the protocol:

$$\varepsilon = \varepsilon_{EC} + \varepsilon_{PA} + \varepsilon_{PE} + \bar{\varepsilon}, \tag{1}$$

where ε_{EC} is the probability that error correction fails, ε_{PA} is the probability that privacy amplification fails, and ε_{PE} is the probability that parameter estimation fails [20]. The parameter $\bar{\varepsilon}$ accounts for the accuracy of estimating the smooth min-entropy, which characterizes the amount of secure information that can be extracted using privacy amplification [16].

The finite-key secure key capacity (measured in bits/photon) for the DO-QKD protocol

can then be written as [16, 17, 18, 19, 20, 21]:

$$r_N = \frac{n}{N}\left(r_\infty - \frac{1}{n}\log\frac{2}{\varepsilon_{EC}} - \frac{2}{n}\log\frac{1}{\varepsilon_{PA}} - (2\log d + 3)\sqrt{\frac{\log(2/\bar{\varepsilon})}{n}}\right). \tag{2}$$

Here r_∞ is the secure key capacity in the asymptotic regime, which was derived in Ref. [14]. N is the number of instances in which Alice and Bob both detect a single photon in a frame. The subtracted terms on the right-hand side of Eq. (2) represent the corrections required in the finite-key length regime. The factor n/N reflects the fact that not all of the signals exchanged and detected by Alice and Bob go toward forming the key since some of the exchanged signals must be sacrificed for parameter estimation. The parameter $n = p^2N$ denotes the number of times that Alice and Bob both chose the time basis. Here, we assumed that measurements made in the 'time basis' are used for the key and measurements made in the dispersed basis are used for parameter estimation. We take $m = (1-p)^2N$ to denote the number of times that Alice and Bob both chose the 'dispersed time basis'. For each value of N, we maximize r_N by optimizing the parameter set $\{\varepsilon_{PA}, \varepsilon_{PE}, \bar{\varepsilon}, p\}$. The security parameter ε is determined beforehand by Alice and Bob's security requirements, and ε_{EC} is fixed by the choice of error correction code. Additionally, the calculation of r_∞ must be modified to include the effects of finite key length on parameter estimation.

2.3 Modified asymptotic secure key capacity and parameter estimation

The asymptotic secure key capacity $r_{\infty,DO}$ was originally calculated [14] as

$$r_\infty = \beta I(A;B) - \chi(A;E), \tag{3}$$

where β is the efficiency of the error correction, $I(A;B)$ is Alice and Bob's mutual information, and $\chi(A;E)$ is Eve's Holevo information. Since Alice and Bob use only measurements made in the 'time basis' for the key, the mutual information is calculated using only the contribution from the 'time basis'.

The Holevo information, accounting for the possibility that Eve could use a biased eavesdropping strategy, is given by

$$\chi(A;E) = S(\rho_E) - p_E\int dt p(t_A = t)S(\rho_{E|t_A=t}) - (1-p_E)\int d\omega p(\omega_A = \omega)S(\rho_{E|\omega_A=\omega}), \tag{4}$$

where $S(\rho)$ is the von Neumann entropy of the quantum state ρ, $p(t_A = t)$ is the probability density for Alice to measure t_A in the 'time basis', $p(\omega_A = \omega)$ is the probability density for Alice to measure ω_A in the 'dispersed time basis', and p_E is the probability with which Eve chooses to eavesdrop in the 'time basis'. We assume that p_E is independent of Alice

and Bob's choice of p. We find that the contributions to the Holevo information from each measurement basis are equal; thus, the Holevo information is unaffected by asymmetric basis selection.

To calculate the Holevo information, Alice and Bob must determine the covariance matrix of their data. The covariance matrix contains two parameters that must be estimated: η, the decrease in correlations, and ϵ, the excess noise. Alice and Bob can obtain values for η and ϵ by using their data to estimate a single parameter, ξ: $\sigma'^2_{cor} = (1+\xi)\sigma^2_{cor}$. ξ quantifies the increase in their photons' correlation time from σ_{cor} to σ'_{cor}, as given in Ref. [15].

Alice and Bob must sample part of their data and use it to make estimates about the entire dataset. In the finite-size regime, it is important to know how well their estimate represents the entire dataset. Since Alice's (Bob's) measured time, T_A (T_B), is a Gaussian-distributed random variable, the difference $(T_A - T_B)$ is also Gaussian-distributed, and thus its variance, $\sigma'_{cor} = \mathrm{VAR}(T_A - T_B)$, can be found using the χ^2 distribution:

$$\chi^2(1-\varepsilon_{PE}, m-1) = (m-1)\frac{\sigma'^2_{cor}}{\sigma^2_{cor}}. \tag{5}$$

An upper bound on σ'_{cor} is then given by [21]:

$$(\sigma'_{cor,max})^2 = \sigma^2_{cor} + \frac{2}{\sqrt{m}}\,\mathrm{erf}^{-1}(1-\varepsilon_{PE})\sigma'^2_{cor}. \tag{6}$$

This bound is valid for the confidence interval $1-\varepsilon_{PE}$. Then, the largest possible estimate for ξ within the confidence interval is

$$\xi_{max} = \frac{(\sigma'_{cor,max})^2}{\sigma^2_{cor}} - 1. \tag{7}$$

Now, Alice and Bob can use their estimate for ξ_{max} to calculate the most pessimistic secure key capacity. Fig. 1 plots the secure key capacity for DO-QKD in the finite regime, using asymmetric basis selection. Finite-size effects only matter for low N, and the most significant effect is due to the parameter estimation.

3 Security using a Franson Interferometer

The team has also been working on security analysis – and a security proof – for high-dimensional quantum key distribution (HD-QKD) that uses time-energy entanglement. We are considering the use of a Franson interferometer – to infer mean-squared frequency error between signal and idler measurements – and a conjugate Franson interferometer – to infer mean-squared timing error between signal and idler measurements. In both cases, the use of a decoy-state protocol will enable those mean-squared errors to be calculated for the biphoton manifold. Then, using a worst-case analysis based on the time-frequency covariance matrix, a bound on Eve's information can be obtained from which a secure key rate can be calculated. This analysis is still underway, but when it is completed it will provide a useful alternative to the mutually-unbiased basis approach using dispersive-optics QKD [15].

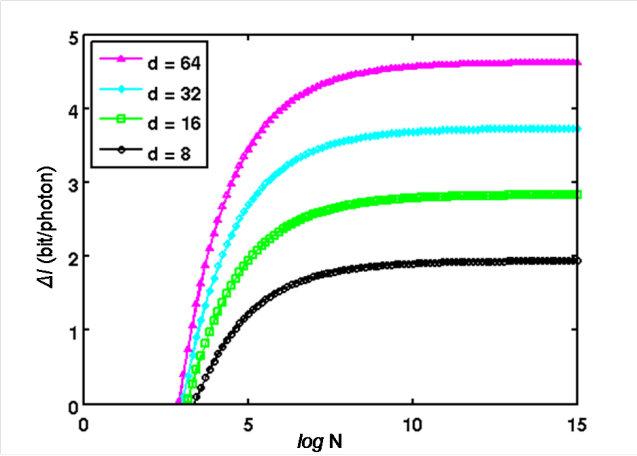

Figure 1: Plot of DO-QKD finite-size secure key capacities assuming Alice and Bob observe $\sigma'_{cor} = 1.1\sigma_{cor}$ and detector jitter $= 2\sigma_{cor}/3$, where σ_{cor} is the correlation time. The security parameter is $\varepsilon = 10^{-5}$, and the failure probability of the error correction is $\varepsilon_{EC} = 10^{-10}$. All other parameters were chosen to match [14]. From top to bottom: $d = 64$, $d = 32$, $d = 16$, $d = 8$.

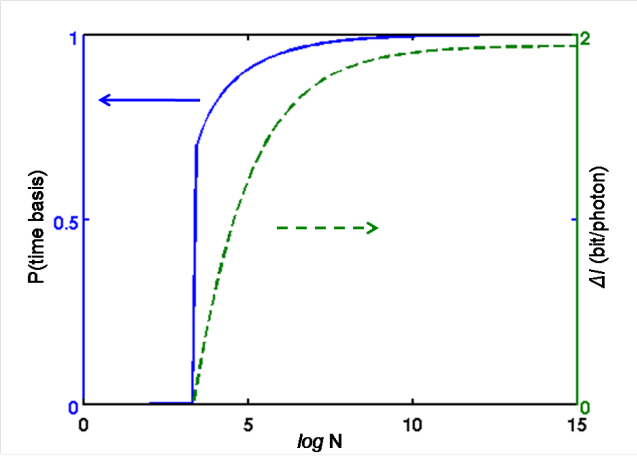

Figure 2: Comparison of DO-QKD finite-size secure key capacity (right) and $p =$ probability of choosing the 'time basis' (left) for $d = 8$.

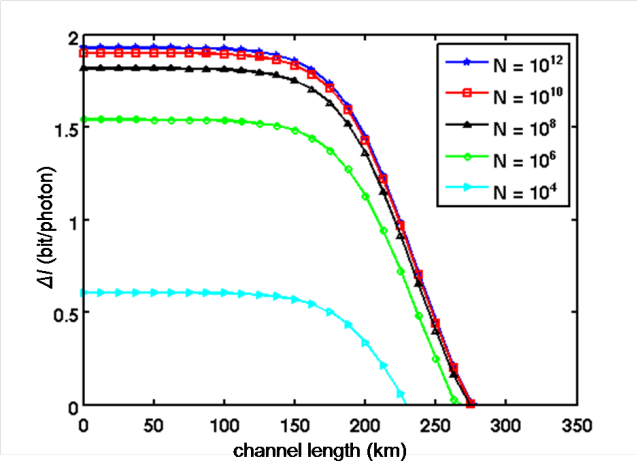

Figure 3: Finite-size secure key capacities versus channel length (loss) for different numbers of signals exchanged, N. $d = 8$ for all; other parameters same as Fig. 1 and [14].

3.1 High-dimensional spectral encoding

With the frequency basis two-photon state, we have now completed the Franson measurement with the 4.2-nm delay line, for Franson interference visibility up to 97.2% for the time-bin measurements. For increasing delay, the falloff in the visibility goes to 93.4% and 86.5% for the higher-order time-bins, matching well with predictions. The correlated two-photon state demonstrates a high-dimensional 16-bin entanglement, through a revival of the Hong-Ou-Mandel interference. Hyperentanglement of the two-photon state has been examined by our team, and will be completed through a higher-dimensional correlation measurement.

4 Experimental QKD Developments

We have completed the following milestones towards the QKD-demos.

- Demonstrated high-dimensional QKD in two different configurations each of which includes both key generation using multiple time bins per measurement time frame and dispersion-compensated Franson-interferometric security checks. One protocol uses SPDC to generate time-energy entangled photon pairs. The protocol, with coincidence detection using InGaAs single-photon detectors and an efficient layered low-density parity-check (LDPC) error-correction code to reconcile the sequence of symbols between Alice and Bob, yields 1.9 secure bits per pair coincidence after privacy amplification. The QKD throughput is currently 83 kbits/s that is limited by the duty cycle and efficiency of the self-differencing InGaAs detectors. Random switching between key generation and security checks is accomplished using passive beam splitters by Alice and by Bob. We expect a 100-fold improvement in the secure key rate if WSi superconducting or high-efficiency NbN nanowire detectors are deployed in our setup.

- The second QKD protocol utilizes weak classical broadband noise from amplified spontaneous emission (ASE) of an unseeded EDFA to prepare time-bin encoded bits through single-photon pulse-position modulation. It also uses SPDC's entangled photons with the same bandwidth as the ASE source for Franson security checks. Random switching between the ASE source and the SPDC source by Alice allows Alice and Bob to perform Franson-interferometric measurements with the SPDC output to monitor the security of the quantum channel. In this hybrid source protocol, we have achieved 2.9 secure bits per photon and a high QKD throughput of 7.3 Mbits/s using InGaAs detectors gated at 1.26 GHz. We estimate that we should be able to achieve a key rate of 33 Mbits/s at ∼6 secure bits per coincidence if WSi detectors are used in the setup, assuming 50 ns reset time and 150 ps timing resolution for the WSi detectors.

4.1 QPIC Development

We measured propagation loss within the waveguide is below 2.5dB/cm; this will be lowered using low-confinement Si waveguides with propagation losses expected below 1 dB/cm. Fig.4.1(b-d) shows several of the of PIC components: a directional waveguide couplers as needed in the arrayed waveguide grating; an inverse tapered polymer-waveguide coupler for efficient mode conversion from an optical fiber to the Si waveguide; and multi-ring add/drop filters.

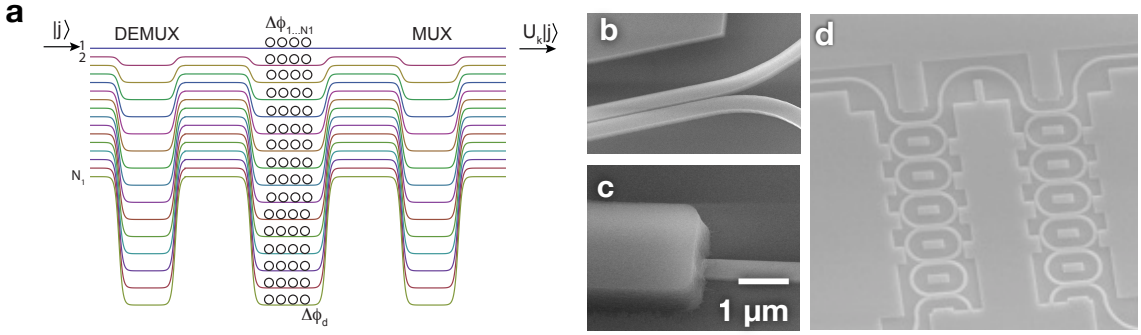

Figure 4: (a) Schematic of a 16-channel dynamic pulse shaper using arrayed waveguide gratings (mux/demux) and controllable phases $\Delta\phi_i$. The PIC includes directional couplers (b), inverse tapered waveguide couplers (c), and add/drop filters consisting of single or coupled rings, as shown in (d).

A fourth-generation PIC has been fabricated with integrated, tunable group velocity dispersion elements. This PIC enables simultaneous DO-QKD channels to operate over up to four frequency channels on the same spatial mode. The PIC is outfit with electrical connections to implement SNSPD detectors on-chip, as recently successfully demonstrated by our team.

In addition, the wavelength-division-multiplexed quantum chip has been prepared. A slight delay on the final etch setup (for the couplers) is due to a missing deep-UV reticle mask, but should be completed by this coming week.

4.2 SNSPD Detector Development

In the last two months we have improved the performance of the detectors and the closed-cycle cryostat used to measure the waveguide-integrated detectors. Waveguide-detectors: We fabricated detectors with sub-25-ps timing jitter and saturated detection efficiency (close to the calculated optical absorption). This was achieved by (1) reducing the exposure time of bare niobium nitride (NbN) to TMAH, a base used as HSQ resist developer which can degrade NbN, and (2) direct heating of the back of the SiNx substrates during the NbN growth process, which resulted in increased critical temperature compared to films grown with the same deposition time but without direct heating. These changes resulted in a higher critical current density (higher signal-to-noise ratio) of our recent detectors.

Fig. 4.2(a) shows the detection efficiency vs bias current for a recent detector based on a parallel-nanowire structure ('series-2-SNAP' based on 84-nm-wide nanowires). The detection efficiency was measured at 2.4 K in a cryogenic probe station using an incoherent CW source. The detector shows a characteristic 'saturation plateau' with a detection efficiency value close to the calculated optical absorption of 11-12% (extracted from simulation results). Due to the high signal-to-noise ratio we could measure a timing jitter of 24ps for these detectors, which is ∼5-10ps lower than the timing jitter values our previous generation of waveguide-detectors. Closed-cycle cryostat: In collaboration with Montana Instruments we replaced four RF channels in the cryostat with low-loss semi-rigid RF cables which provided 2-6dB/m attneuation at 0.5-5GHz, a resulting in a significant improvement of the signal amplitude compared to the previous RF lines (13-40dB/m at 0.5-5GHz). Furthermore, as shown in Fig. 1(c), we measured the detector signal using miniature coaxial lines directly connected to the printed circuit board, which resulted in an improved noise base of the signal compared to the previous solution which relied on RF cables that were directly soldered to the PCB. Harnessing the higher signal-to-noise ratio we recently measured sub-30-ps timing jitter (Figure 1(d)) in the closed-cyle cryostat. For these measurements the detectors were front-illuminated with a mode-locked picosecond-pulsed laser. We are currently preparing a photonic integrated chip with waveguide-detectors which will allow us to couple light into the detector through the waveguides.

5 Publications and Presentations

Tian Zhong of MIT presented a poster on the dispersion compensation for the Franson interferometer at the 11th Conference on Quantum Communication, Measurement, and Computing in Vienna, Austria, August 2012.

5.1 Journal Publications

- Directional free-space coupling from photonic crystal waveguides, C.-C. Tsai, J. Mower, and D. Englund, Optics Express 19 (21), 20586-96 (2011)
- Efficient generation of single and entangled photons on a silicon photonic integrated chip, J. Mower and D. Englund, Phys. Rev. A 84, 052326 (2011)

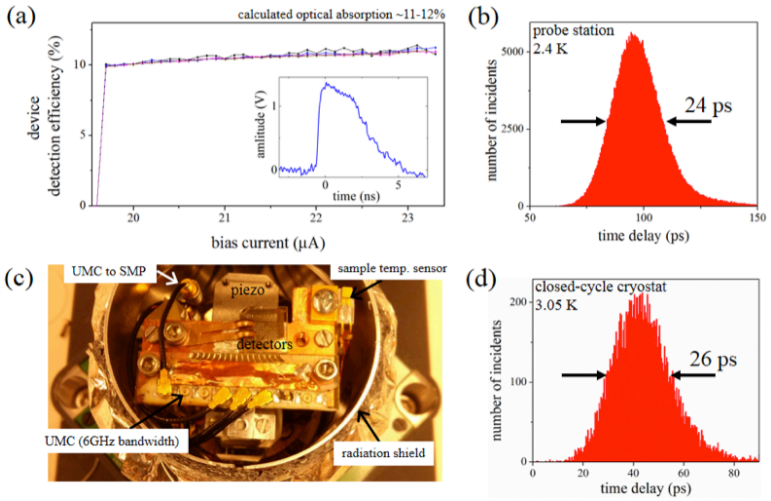

Figure 5: (a) Back-illuminated device detection efficiency vs bias current for a series-2-SNAP based on ∼84-nm-wide nanowires. The incident photon flux was varied between 830 k photons/second (black) and 13 M photons/second (brown). The inset shows the voltage trace of the output pulse at a bias current of 22μA. (b) Instrument response function (IRF) of the same detector as in (a) biased at 22μA. (c) Image of sample-holder with detector chip and miniature RF (UMC) connections. (d) IRF of a detector using the setup shown in (c). The detector reached ∼26ps FWHM timing jitter when biased at 22 μA.

- Wavelength Division Multiplexed Quantum Key Distribution, J. Mower, F. Wong, J. Shapiro, D. Englund, ArXiv:1110.4867 (2011)
- Zero phase delay in negative-index photonic crystal superlattices, S. Kocaman, M.S. Aras, P. Hsieh, J. F. McMillan, C. G. Biris, N. C. Panoiu, M. B. Yu, D. L. Kwong, A. Stein, and C. W. Wong, Nature Photonics 5, 499 (2011).
- High-dimensional quantum key distribution using dispersive optics, J. Mower, P. Desjardins, J. H. Shapiro, D. Englund, Phys. Rev. Lett. A 87 (2013).
- Private-Capacity Bounds for Bosonic Wiretap Channels, Ligong Wang, Jeffrey H. Shapiro, Nivedita Chandrasekaran, and Gregory W. Wornell, ArXiv:1202.1126 (2012)
- "Efficient single-spatial-mode periodically poled $KTiOPO_4$ waveguide source for high-dimensional entanglement-based quantum key distribution." Co-authors include Alessandro Restelli and Josh Biefang of NIST. Manuscript is under NIST review; we expect to submit it to Optics Express in early September.
- Nanophotonic Filters and Integrated Networks in Flexible 2D Polymer Photonic Crystals, X. Gan, H. Clevenson, C.-C. Tsai, L. Li, and D. Englund, to appear in Nature Scientific Reports (2013)

5.2 Conference Papers

- T. Zhong, F. N. C. Wong, A. Restelli, and J. C. Biefang, "Efficient single-spatial-mode PPKTP waveguide source for high dimensional entanglement-based QKD," to be presented at CLEO/QELS 2012, paper JTh1K3.
- eT. Zhong and F. N. C. Wong, "Franson interferometry with 99.6% visibility via fiberoptic dispersion engineering," in 11th International Conference on Quantum Communication, Measurement and Computing, Vienna, Austria, July 2012, paper accepted for presentation.
- D. Englund and J. Mower, "Quantum Optics on Silicon Photonic Chips", Invited Paper at Frontiers In Optics (San Jose, CA, Oct. 18, 2011)
- On High-Efficiency Optical Communication and Key Distribution, Yuval Kochman and Gregory W. Wornell, ITA, San Diego (2012)
- Private-Capacity Bounds for Bosonic Wiretap Channels, Ligong Wang, Jeffrey H. Shapiro, Nivedita Chandrasekaran, and Gregory W. Wornell, submitted to IEEE International Symposium on Information Theory (2012)
- F. N. C. Wong, "Time-energy entangled waveguide source for high-dimensional QKD," in Laser Science XXVII, San Jose, CA, October 2011, invited paper $LTuF_4$.
- J. Mower and D. Englund, "High-dimensional quantum key distribution using dispersive optics," submitted for Frontiers in Optics, Rochester, NY, 2012

References

[1] H. Bechmann-Pasquinucci and W. Tittel. Quantum cryptography using larger alphabets. *Phys. Rev. A*, 61:062308, May 2000.

[2] C. H. Bennett and G. Brassard. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179. IEEE, New York, 1984.

[3] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[4] Nicolas J. Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin. Security of Quantum Key Distribution Using d-Level Systems. *Phys. Rev. Lett.*, 88:127902, Mar 2002.

[5] Lijian Zhang, Christine Silberhorn, and Ian A. Walmsley. Secure Quantum Key Distribution using Continuous Variables of Single Photons. *Phys. Rev. Lett.*, 100:110504, Mar 2008.

[6] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Quantum Cryptography Using Entangled Photons in Energy-Time Bell States. *Phys. Rev. Lett.*, 84:4737–4740, May 2000.

[7] R. T. Thew, A. Acín, H. Zbinden, and N. Gisin. Bell-Type Test of Energy-Time Entangled Qutrits. *Phys. Rev. Lett.*, 93:010503, Jul 2004.

[8] Irfan Ali-Khan, Curtis J. Broadbent, and John C. Howell. Large-Alphabet Quantum Key Distribution Using Energy-Time Entangled Bipartite States. *Phys. Rev. Lett.*, 98:060503, Feb 2007.

[9] R. T. Thew, S. Tanzilli, W. Tittel, H. Zbinden, and N. Gisin. Experimental investigation of the robustness of partially entangled qubits over 11 km. *Phys. Rev. A*, 66:062304, Dec 2002.

[10] B. Qi. Single-photon continuous-variable quantum key distribution based on the energy-time uncertainty relation. *Optics letters*, 31(18):2795–2797, 2006.

[11] Alois Mair, Alipasha Vaziri, Gregor Weihs, and Anton Zeilinger. Entanglement of the orbital angular momentum states of photons. *Nature*, 412(6844):313–316, 2001.

[12] Alipasha Vaziri, Gregor Weihs, and Anton Zeilinger. Experimental Two-Photon, Three-Dimensional Entanglement for Quantum Communication. *Phys. Rev. Lett.*, 89:240401, Nov 2002.

[13] G. Molina-Terriza, A. Vaziri, J. Řeháček, Z. Hradil, and A. Zeilinger. Triggered Qutrits for Quantum Communication Protocols. *Phys. Rev. Lett.*, 92:167903, Apr 2004.

[14] Jacob Mower, Zheshen Zhang, Pierre Desjardins, Catherine Lee, Jeffrey H. Shapiro, and Dirk Englund. High-dimensional quantum key distribution using dispersive optics. *Phys. Rev. A*, 87:062322, Jun 2013.

[15] Jacob Mower, Zheshen Zhang, Pierre Desjardins, Catherine Lee, Jeffrey H. Shapiro, and Dirk Englund. High-dimensional quantum key distribution using dispersive optics. *Phys. Rev. A*, 87:062322, Jun 2013.

[16] Valerio Scarani and Renato Renner. Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing. *Phys. Rev. Lett.*, 100:200501, May 2008.

[17] Lana Sheridan and Valerio Scarani. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A*, 82:030301, Sep 2010.

[18] Lana Sheridan and Valerio Scarani. Erratum: Security proof for quantum key distribution using qudit systems [Phys. Rev. A 82, 030301(R) (2010)]. *Phys. Rev. A*, 83:039901, Mar 2011.

[19] Raymond Y Q Cai and Valerio Scarani. Finite-key analysis for practical implementations of quantum key distribution . *New J. Phys.*, 11:045024, 2009.

[20] Lana Sheridan, Thinh Phuc Le, and Valerio Scarani. Finite-key security against coherent attacks in quantum key distribution. *New J. Phys.*, 12(12):123019, 2010.

[21] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A*, 81:062343, Jun 2010.

[22] Hoi-Kwong Lo, H. F. Chau, and M. Ardehali. Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security. *Journal of Cryptology*, 18:133–165, 2005.

[23] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002.